UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE DROPBOX ACCOUNT ASSOCIATED WITH THE EMAIL ADDRESS SINGLEMALTGRUX@GMAIL.COM	)))))	No. 1:22-MJ-180-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. This affidavit is made in support of an application for the search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox Inc., to disclose to the government records and other information in its possession (including the content of communications) pertaining to the subscriber or users associated with the email address "singlemaltgrux@gmail.com" (hereinafter referred to as the "SUBJECT ACCOUNT"), which are stored at the premises owned, maintained, controlled, or operated by Dropbox Inc. The information to be searched is described in the following paragraphs and in Attachment A. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. This affidavit is based in part on information that I learned from discussions with other law enforcement officers and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and

instrumentalities of the violation of 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B), are presently located in the SUBJECT ACCOUNT.

AGENT BACKGROUND

3. I am a detective with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I have also completed HSI's Task Force Officer Course. I hold a bachelor's degree in criminal justice, with a minor in computer science and victimology, from Endicott College.

4. Since November 2019, I have been assigned to the Special Investigations Division as a member to the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a TFO, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a TFO and a member of the ICAC, I investigate criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have also participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations and using undercover personas on various social media applications for proactive

investigations. I have personally conducted numerous online undercover investigations using social media applications such as KIK messenger, Grindr, WhatsApp, Whisper, and MeetMe. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics. In the course of investigating crimes related to the sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous online child sexual exploitation investigations and am very familiar with the tactics used by child pornography offenders who collect child pornographic material and those who seek to exploit children.

5. In addition, over the course of this investigation, I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses.

STATUTORY AUTHORITY

6. This application is part of an investigation into Scott Currier for the alleged knowing transportation, receipt, and possession of child pornography. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly transporting child pornography using any means or facility of interstate or foreign commerce. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving and distributing any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have

been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States…that- has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

BACKGROUND ON DROPBOX AND NCMEC'S CYBER TIP LINE

8. Dropbox Inc., commonly referred to as Dropbox, is a file hosting service headquartered in San Francisco, California that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox offers free services to users in which they can store 2GB of information along with various plans which require a user to pay. In order to use Dropbox services, an individual must register for an account during which time they must provide their first name, last name, email address, and a password. Once an individual has an account they can store various forms of media on the account and share links which can contain the media they store. Users can also download links which contain other user's media.

9. The National Center for Missing & Exploited Children is a private, nonprofit organization established in 1984 by the United States Congress. NCMEC's mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. In support of this mission, NCMEC operates the Cyber Tip line. Under United States federal law (18 U.S. Code § 2258A), U.S.-based electronic service providers (ESPs), such as Dropbox, are

required to report instances of apparent child pornography that they become aware of on their systems to NCMEC.

PROBABLE CAUSE

Background Information:

10. On April 5, 2000, Scott Christopher Currier was convicted for aggravated sexual assault and felonious sexual assault in Strafford County Superior Court. As a result of these convictions, Currier is required to register as a sex offender in New Hampshire.

11. In March 2018, Currier was under court supervision by the United States Probation Office. During a cursory examination of Currier's cell phone, the Probation Officer observed a video file of potential child sexual exploitation in the Dropbox application.

12. On September 18, 2018, HSI Special Agents Michael Perrella and Ronald Morin conducted a voluntary interview with Currier at his parents' residence in Dover, New Hampshire. During the interview, Currier discussed his use of a Dropbox account, and he further advised that his cell phone photos were automatically backed up to the Dropbox account. Currier informed agents that within chat rooms he was a part of he had observed "younger shit," which he furthered described as pubescent and prepubescent pornography depicting both boys and girls. Currier also informed agents that every time he discovered an image, he deleted it, and believed he had deleted approximately thirty images. Ultimately, Currier was only charged with a violation of his federal probation.

Current Investigation:

13. On June 08, 2022, Dunbarton Police Sergeant Brian Tyler was assigned to investigate Cyber Tip 123083989 reported by Dropbox, Inc. In reporting the Cyber Tip, Dropbox identified the suspect by email address (singlemaltgrux@gmail.com) and screen/username (Chris

Currier). Dropbox also provided IP addresses used to log into the account and one file (filename "2015-12-05 11.44.02.mp4") from the account which Dropbox advised was publically available and had been reviewed by the company. File name "2015-12-05 11.44.02.mp4" is a one-minute and thirty-one second video depicting a pubescent female engaging in masturbation and exposing her vagina and anus to the camera.

14. On June 14, 2022, Sgt. Tyler obtained a state search warrant for the SUBJECT ACCOUNT. After Sgt. Tyler received the search warrant response from Dropbox for the SUBJECT ACCOUNT, he provided copies to me. Based upon my review of the Dropbox response, I observed that the SUBJECT ACCOUNT was organized into twenty-seven different folders[1], and I determined that over 100 files qualify as child sexual exploitation material. Below is a description of two of the files that I identified as child sexual exploitation videos during my review:

a. Filename "1fab09cc-c891-4f42-ba30-466ffa15f57b.mp4" is a 13-second video depicting an adult male and an infant. The adult male inserted a portion of his penis into the infant's mouth while rubbing the other portion of his penis with his hand. The infant appears to be crying in this video.

b. Filename "54df7058-0ae7-423a-81e5-3dd511149130.mp4" is a 59-second video depicting an adult male and a prepubescent female in a bathtub. The adult male is sitting with his legs spread, and the prepubescent female is positioned between his legs. The prepubescent female is using her hands to stimulate his penis.

[1] The names for the folders included: Camera Uploads, Camera Uploads3, camera-uploads2, Elizabeth (leah) giss, fingering & more, kik vids, kik vids 2, kik2, lez, lot of vids, Mine, mystery, N2, new vids2, Nudes, Num.1, stuffy, testx1x, untitled folder, Vault, Video2, Videos and stuff, vids (1), white2, x, ybj, Youngz.

15. In June 2022, Sgt. Tyler obtained a state search warrant for the email account "singlemaltgrux@gmail.com," which is the email address associated with the SUBJECT ACCOUNT. From the Gmail search warrant results, Sgt. Tyler identified photographs of Scott Christopher Currier, including one image of Currier holding his New Hampshire driver's license next to his face. In addition, Sgt. Tyler recognized that the Dropbox returns for the SUBJECT ACCOUNT included photographs of Currier within a folder titled "Camera Uploads."

16. On July 27, 2022, law enforcement executed a federal search warrant for Currier's person, his vehicle, and his residence in Dunbarton, New Hampshire. Special Agent Derek Dunn and I conducted a voluntary interview with Currier after he waived the Miranda Rights. Currier admitted that the SUBJECT ACCOUNT belonged to him, but he denied storing any child sexual exploitation materials on the SUBJECT ACCOUNT.

17. Following execution of the search warrant, I again reviewed the results for the SUBJECT ACCOUNT from the state Dropbox search warrant. During this review, I observed there was no upload log provided with the search warrant results. The upload log would show when files in the account were added and how they were added.

18. On August 02, 2022, I emailed Dropbox's legal compliance department regarding the upload logs, and I received the following response:

> Hello,
>
> Thank you for your email. The search warrant request 00024583 did not request an upload log. Dropbox will only provide data, if available, that is specifically requested in the legal process document. Please review our Information for Law Enforcement for additional information on serving requests to Dropbox.

In response, I advised that I would seek and submit an updated search warrant. Dropbox's legal compliance department acknowledged my response and provided instructions for submitting the

updated search warrant via Dropbox's Law Enforcement and Government Online Submission System.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

19. In addition to the upload logs for the SUBJECT ACCOUNT, out of an abundance of caution and in order to have complete results, the requested search warrant seeks to obtain information that may have been produced by Dropbox in response to the state search warrant.

20. The evidence believed to be located within the SUBJECT ACCOUNT is listed in Attachment B, which is incorporated by reference as if fully set forth herein, and is believed to be contained on servers and digital storage media maintained by and under the control of Dropbox Inc.

21. This application seeks a warrant to search all responsive records and information under the control of Dropbox Inc., a provider subject to the jurisdiction of this court, regardless of where Dropbox has chosen to store such information[2]. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Dropbox's possession, custody, or control, regarding of whether such communication, records, or other information is stored, held, or maintained outside the United States.

22. Pursuant to 18 U.S.C. § 2703(g), this application and affidavit for a search warrant seeks authorization to require Dropbox Inc., and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to

[2] It is possible that Dropbox, Inc. stores some portion of the information sought outside of the United States. Under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), the Stored Communications Act was amended to require that communications providers in the United States respond to legal process and return relevant data regardless of the location of the servers containing the data.

Dropbox Inc., with direction that they identify the account described in Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section 1 of Attachment B to this affidavit. The search warrant will direct Dropbox Inc., to create an exact copy of the specified account and records.

23. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachments B for seizure.

24. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachments B to the warrant.

25. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of

messages and documents that identify any users of the SUBJECT ACCOUNT and messages sent or received in temporal proximity to incriminating messages that provide context to the incriminating communications.

CONCLUSION

26. Based on the foregoing, I request that the court issue the proposed search warrant authorizing a search of the SUBJECT ACCOUNT specified in Attachment A for the items more fully described in Attachment B.

Dated: August 10, 2022

Respectfully Submitted,

/s/ Adam Rayho
Adam Rayho
Task Force Officer
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire
Date: August 10, 2022

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Dropbox Account associated with the email address "singlemaltgrux@gmail.com" (the "SUBJECT ACCOUNT"), that is stored at premises owned, maintained, controlled, or operated by Dropbox Inc., a company based in San Francisco, California.

Notwithstanding Title 18, United States Code, Section 2252A or similar statute or code, Dropbox Inc., shall disclose responsive data, if any, by delivering encrypted files to the United States Attorney's Office, District of New Hampshire, c/o AUSA Kasey Weiland, 53 Pleasant Street, 4th Floor, Concord, New Hampshire 03301.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received via Dropbox, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Records, data, and images relating to the possession, distribution, or receipt of materials which constitute child erotica or child pornography (including any files – still images or video files – depicting child pornography).

(b) Records, data, and images relating to the identity of the person(s) who created, used, or communicated with the Dropbox account, including records that help reveal the whereabouts of such person(s), such as, but not limited to, first name, last name, middle name, e-mail address, e-mail password, address, phone number, DOB, driver's license number, bank name, bank account number, bank routing number, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

(c) Records and data relating to the identity of the person(s) who communicated with the Dropbox account regarding the possession, distribution, or receipt of materials that constitute child erotica or child pornography, including records that help reveal their whereabouts.